(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2002 年1 月10 日 (10.01.2002)

PCT

(10) 国際公開番号
WO 02/03271 A1

(51) 国際特許分類[7]: G06F 17/60, G06K 19/07

(21) 国際出願番号: PCT/JP00/04447

(22) 国際出願日: 2000 年7 月4 日 (04.07.2000)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): 株式会社 日立製作所 (HITACHI, LTD.) [JP/JP]; 〒101-8010 東京都千代田区神田駿河台四丁目6番地 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 原口政敏 (HARAGUCHI, Masatoshi) [JP/JP]; 〒244-0003 神奈川県横浜市戸塚区戸塚町5030番地 株式会社 日立製作所 ソフトウェア事業部内 Kanagawa (JP).

(74) 代理人: 平木祐輔, 外 (HIRAKI, Yusuke et al.); 〒105-0001 東京都港区虎ノ門一丁目17番1号 虎ノ門5森ビル3F Tokyo (JP).

(81) 指定国 (国内): AU, JP, US.

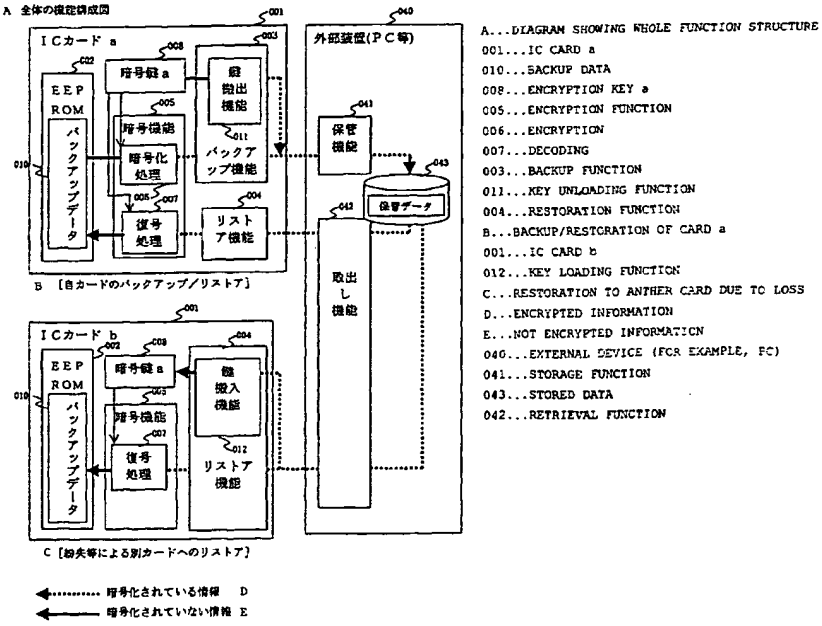
(84) 指定国 (広域): ヨーロッパ特許 (DE, FR, GB).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: IC CARD, METHOD FOR BACKING UP IC CARD, AND RESTORING METHOD

(54) 発明の名称: ICカード、ICカードのバックアップ方法及びリストア方法



A...DIAGRAM SHOWING WHOLE FUNCTION STRUCTURE
001...IC CARD a
010...BACKUP DATA
008...ENCRYPTION KEY a
005...ENCRYPTION FUNCTION
006...ENCRYPTION
007...DECODING
003...BACKUP FUNCTION
011...KEY UNLOADING FUNCTION
004...RESTORATION FUNCTION
B...BACKUP/RESTORATION OF CARD a
001...IC CARD b
012...KEY LOADING FUNCTION
C...RESTORATION TO ANTHER CARD DUE TO LOSS
D...ENCRYPTED INFORMATION
E...NOT ENCRYPTED INFORMATION
040...EXTERNAL DEVICE (FOR EXAMPLE, PC)
041...STORAGE FUNCTION
043...STORED DATA
042...RETRIEVAL FUNCTION

(57) Abstract: An IC card safe in security is backed up. Data is encrypted (005) using an encryption key (008) uniquely given to a card (001) and provided only to the inside of the card (001) to back up (003) the data. The data backed up is decoded in the same card and restored. The encryption key uniquely given to the card is encrypted using a common encryption key provided only in cards and common to the cards and backed up together with the data. The encryption key uniquely given to the card and backed up is decoded using the card common encryption key in another card, and the data backed up is decoded in the another card and restored.

WO 02/03271 A1

[続葉有]

(57) 要約:

セキュリティ面で安全なＩＣカードのバックアップを実現する。カード(001)内だけに存在するカード固有の暗号鍵(008)を用いて暗号化して(005)バックアップする(003)。バックアップしたデータは同じカード内で復号してリストアする。さらに、カード内だけに存在するカード間で同一な共通暗号鍵を用いてカード固有の暗号鍵を暗号化して一緒にバックアップし、このバックアップしたカード固有の暗号鍵を別カード内でカード共通暗号鍵を用いて復号することにより、バックアップデータを別カード内で復号してリストアする。

明　細　書

ＩＣカード、ＩＣカードのバックアップ方法及びリストア方法

技術分野

この発明は、ＩＣカードに関し、特にＩＣカードのメモリ内容をバックアップする方法及びリストアする方法に関する。

背景技術

ＩＣカード内の情報を他のＩＣカードに復元する技術として、特開平９－１７９９２１号公報に記載のものがある。この技術によると、利用者は電子商取引情報（例えば電子マネー）を保有する取引き用ＩＣカードと金銭出納の履歴を記録するバックアップ用ＩＣカードの２つを所持し、取引き用ＩＣカードの破損・紛失時にバックアップ用ＩＣカードの履歴から別のＩＣカードへ取引き用ＩＣカード内の電子商取引情報の復元を図る。

上記従来技術では、利用者はＩＣカードをペアで所有する必要があり実用面から利用者の負担が大き過ぎること、またカードを両方共紛失した場合は復元できないという問題がある。また復元できる情報は、バックアップ用ＩＣカードに記録できる履歴の範囲に限定されるという問題もある。

ＩＣカードは、ＩＣチップ技術の進歩に伴ないメモリ容量の拡大とＣＰＵ能力の向上により、その用途は金融、流通、通信、交通、エンターテイメント、行政など社会生活の幅広い分野に採用される。また、より便利にするため１枚のＩＣカードで複数の用途に適用すること、すなわち複数のアプリケーションを搭載することが必要となる。また、利用者自身によるアプリケーションのロードや削除ができることも必要となる。１枚のＩＣカードが複数の用途に利用され、また格納される重要な情報が多くなると便利になる反面、ＩＣカードの破損、紛失等による損失面が大きな問題となる。

また、電子マネー、ポイントなどのバリュー（値そのものが経済的価値を持つデータ）を扱うカードアプリケーションをバックアップ対象にする場合、リスト

アするとバリューがバックアップ時点に戻ってしまうためバックアップが適用できないという問題がある。

発明の開示

本発明の第一の目的は、ＩＣカードのメモリに格納されている情報（プログラムコード、データ、プログラムの制御情報等）を暗号化してカード外の装置にバックアップし、必要な時点で同一のカードあるいは別カード内で復号してリストアすることによりセキュリティ面で安全なバックアップを実現することにある。

また、本発明の第二の目的は、バックアップの対象となるメモリの変更されている部分だけのバックアップとリストアを可能にすることで処理時間の短縮と格納媒体容量の削減を図ることにある。

また、本発明の第三の目的は、電子マネー、ポイントなどのバリューを扱うカードアプリケーション（ＡＰ）をバックアップ対象にする場合、ＡＰが該バリューを取り扱う前にＡＰ自身で該バリューを初期化する手段を備えることによって、バリューがバックアップ時点に戻ってしまう問題を解決し、バックアップの適用範囲を広げることにある。

前記第一の目的を達成するため本発明では、カード内だけに存在するカード固有の暗号鍵を用いて暗号化してバックアップし、またバックアップしたデータは同じカード内で復号してリストアする方法を採用する。この方法は、カード外での復号を必要としない方法であるため安全性が高い。

また、別カードに対するリストアは、カード内だけに存在するカード間で同一なカード共通暗号鍵を用いてカード固有の暗号鍵を暗号化してバックアップデータの一部としてバックアップし、またバックアップしたカード固有の暗号鍵を別カード内でカード共通暗号鍵を用いて復号し、さらにバックアップデータは当該別カード内で前記カード固有の暗号鍵を用いて復号することで実現する。このように、別カードにリストアする場合でもカード外での復号を必要としない方法であるため安全性が高い。

前記第二の目的を達成するため本発明では、メモリ内容の変更の有無を固定長(ページ)単位ごとに判断できる手段を備え、この手段を利用して変更されている

ページだけのバックアップとリストアを実現する。これによりバックアップとリストアのための処理時間の短縮と格納媒体容量の削減ができる。

前記第三の目的を達成するため本発明では、ＩＣカード内のプログラムをオペレーティングシステム（ＯＳ）とカードアプリケーション（ＡＰ）とに別けて構成させる場合、このバックアップする機能をＯＳの機能として実現する。これにより、複数搭載されるＡＰへの負担を強いることなくＯＳ単独でバックアップを行うことができる。また、電子マネー、ポイント等のバリューを持つデータを扱うＡＰのリストアを実行した場合、ＯＳがＡＰにリストアを実行したことを通知する手段と、ＡＰがバリューを取り扱う前にバリューを初期化して例えばゼロにする手段を備える。

このリストアの実行時にＩＣカード内のバリューを初期化するという方法は、利用者が本物の財布を紛失したらその中のお金も無くなるという考え方と、同一カードにリストアするケースではリストア前に利用者自身で当該ＩＣカード内に残っているバリューを一旦使い切ってしまうあるいは他の媒体等に移すことができるためバリューを初期化することによる損失を回避できるという考え方を基にしている。

すなわち、本発明の一態様によるＩＣカードは、暗号鍵と、暗号化処理及び復号処理を行う暗号機能と、前記暗号鍵を用いて暗号機能の暗号化処理でＩＣカードのメモリに格納されている情報を暗号化したバックアップデータを搬出するバックアップ機能と、搬入した暗号化されたバックアップデータを前記暗号鍵を用いて暗号機能の復号処理で復号しメモリにリストアするリストア機能とを備えることを特徴とする。

本発明の一態様によるＩＣカードは、また、当該ＩＣカードに固有の暗号鍵と、複数のＩＣカードに共通の暗号鍵と、暗号化処理及び復号処理を行う暗号機能と、前記固有の暗号鍵を用いて暗号機能の暗号化処理でＩＣカードのメモリに格納されている情報を暗号化したバックアップデータと共通の暗号鍵を用いて暗号機能の暗号化処理で暗号化した固有の暗号鍵とを含む情報を搬出するバックアップ機能とを備えることを特徴とする。

本発明の一態様によるＩＣカードは、第１の暗号鍵と、暗号鍵を用いて復号処

理を行う暗号機能と、搬入した暗号化された情報から第１の暗号鍵を用いて暗号機能の復号処理で第２の暗号鍵を復号する機能と、搬入した暗号化された情報から第２の暗号鍵を用いて暗号機能の復号処理でバックアップデータを復号しメモリにリストアするリストア機能とを備えることを特徴とする。

本発明の一態様によるＩＣカードは、また、ＩＣカードに固有の暗号鍵と、複数のＩＣカードに共通の暗号鍵と、暗号化処理及び復号処理を行う暗号機能と、ＩＣカードに固有の暗号鍵を用いて暗号機能の暗号化処理でＩＣカードのメモリに格納されている情報を暗号化したバックアップデータと共通の暗号鍵を用いて暗号機能の暗号化処理で暗号化したＩＣカードに固有の暗号鍵とを含む情報を搬出するバックアップ機能と、搬入した暗号化された情報から共通の暗号鍵を用いて暗号機能の復号処理でＩＣカードに固有の暗号鍵を復号する機能と、復号したＩＣカードに固有の暗号鍵を用いて暗号機能の復号処理で復号したバックアップデータをメモリにリストアするリストア機能とを備えることを特徴とする。

前記バックアップデータにはＩＣカードを識別する個々のＩＣカードに固有の識別情報を含ませることができる。

本発明ののの一態様によるＩＣカードは、リストアを実行したことを示す情報を保持し、その情報をカードアプリケーションに通知する機能を有するオペレーティングシステムを備えることができる。リストアを実行したことを示す情報は、例えばフラグによって保持することができる。

アプリケーションが値そのものが経済的価値を有するデータ（バリュー）を扱うアプリケーションの場合、アプリケーションはリストアを実行したことを示す情報を受け取ったときバリューを初期化する処理を行うのが好ましい。

本発明の一態様によるＩＣカードは、また、当該ＩＣカードに固有の暗号鍵と、複数のＩＣカードに共通の暗号鍵と、暗号化処理及び復号処理を行う暗号機能と、共通の暗号鍵を用いて暗号機能の暗号化処理で暗号化した固有の暗号鍵を搬出する鍵搬出機能と、搬入した情報から共通の暗号鍵を用いて暗号機能の復号処理でＩＣカードに固有の暗号鍵を復号する鍵搬入機能とを備えることを特徴とする。

本発明の一態様によるＩＣカードのバックアップ方法は、ＩＣカードのメモリ内容をＩＣカード外の装置にバックアップするＩＣカードのバックアップ方法に

おいて、メモリ内容をＩＣカード内だけに存在するＩＣカードに固有の暗号鍵を用い暗号化してバックアップデータとしてＩＣカード外の装置に搬出することを特徴とする。

本発明の一態様によるＩＣカードのメモリ内容リストア方法は、外部装置にバックアップしたＩＣカードのメモリ内容をＩＣカードにリストアするＩＣカードのメモリ内容リストア方法において、外部装置から搬入した暗号化されたバックアップデータをＩＣカード内だけに存在するＩＣカードに固有の暗号鍵を用い復号してメモリにリストアすることを特徴とする。

バックアップデータにＩＣカードを識別する識別情報を含ませ、リストア時にバックアップデータに含まれている識別情報とリストアするＩＣカードの識別情報の一致をチェックするようにしてもよい。

本発明の一態様による、第１のＩＣカードのメモリ内容を外部装置にバックアップし、バックアップしたメモリ内容を第２のＩＣカードのメモリにリストアする方法は、第１のＩＣカード内だけに存在する第１のＩＣカードの固有の暗号鍵を第１のＩＣカード内で第１および第２のＩＣカードに共通の暗号鍵を用いて暗号化したデータと、第１のＩＣカードのメモリ内容を第１のＩＣカードに固有の暗号鍵を用いて第１のＩＣカード内で暗号化したデータとを含むバックアップデータを第１のＩＣカードから外部装置に搬出するステップと、第２のＩＣカードで外部装置から前記バックアップデータを搬入するステップと、搬入したバックアップデータから、ＩＣカード内だけに存在する共通の暗号鍵を用いて、第２のＩＣカード内で第１のＩＣカードに固有の暗号鍵を復号するステップと、搬入したバックアップデータから、復号した第１のＩＣカードに固有の暗号鍵を用いて、第２のＩＣカード内で第１のＩＣカードのメモリ内容を復号するステップと、復号した第１のＩＣカードのメモリ内容を第２のＩＣカードのメモリにリストアするステップとを含むことを特徴とする。

このとき、第１のＩＣカードのメモリ内容をリストアすべきＩＣカードの識別情報を予め取得してバックアップデータに付加しておき、バックアップデータに付加された識別情報と第２のＩＣカードが保持している識別情報の一致をチェックするようにしてもよい。

本発明の一態様による、ＩＣカードのメモリ内容を外部装置にバックアップし、バックアップしたメモリ内容をＩＣカードのメモリにリストアする方法は、バックアップ対象メモリの内容変更の有無をメモリの分割単位（ページ）ごとに判断し、変更されているページだけのバックアップとリストアをすることを特徴とする。

このとき、外部装置は、バックアップデータの管理情報としてバックアップの順序番号と当該バックアップが全体バックアップか変更ページだけの部分バックアップかの情報を保管しておき、この管理情報を用いて一連のバックアップデータを一括してリストアするようにすることができる。

本発明の一態様による、ＩＣカードのメモリ内容を外部装置にバックアップし、バックアップしたメモリ内容をＩＣカードのメモリにリストアする方法は、ＩＣカード内のプログラムをオペレーティングシステムとアプリケーションプログラムとに別けて構成し、バックアップ機能及びリストア機能をオペレーティングシステムの機能として実現することを特徴とする。アプリケーションプログラムが電子マネー、ポイント等のバリューを持つとき、オペレーティングシステムがバックアップとリストアを実行した場合、オペレーティングシステムがアプリケーションプログラムにリストアの実行を通知し、リストアの実行を通知されたアプリケーションプログラムはバリューの利用前に当該バリューを初期化することが好ましい。

本発明の一態様によるＩＣカードにプログラムを格納する方法は、ＩＣカードの外部に格納されたプログラムをＩＣカードに格納するとき、該プログラムがＩＣカードの外部から読み込まれたことを認知するプログラムからその旨を示す情報を受け取り、その情報に基づいてＩＣカード内の予め定められた領域に特定の値をセットすることを特徴とする。この方法によると、ＩＣカードに外部から格納されるプログラムが電子マネーやポイント等のバリューを扱うアプリケーションプログラムであるとき、ＩＣカードの外部からプログラムとともに読み込まれたバリューを無効にし、ＩＣカード内に設定されるバリューを特定の値、例えばゼロ等の初期値を設定することによって、不正なバリューの生成を禁止することができる。

本発明の一態様によるＩＣカードにプログラムを格納する方法は、ＩＣカードの外部に格納されたプログラムをＩＣカードに格納するとき、該プログラムがＩＣカードの外部から読み込まれたことを認知する回路からその旨を示す情報を受け取り、その情報に基づいてＩＣカード内の予め定められた領域に特定の値をセットするようにしてもよい。この方法によっても、ＩＣカードに外部から格納されるプログラムが電子マネーやポイント等のバリューを扱うアプリケーションプログラムであるとき、ＩＣカードの外部からプログラムとともに読み込まれたバリューを無効にし、ＩＣカード内に設定されるバリューを特定の値、例えばゼロ等の初期値とすることによって、不正なバリューの生成を禁止することができる。

本発明の一態様によるＩＣカードにアプリケーションプログラムをリストアする方法は、ＩＣカードの外部に格納されたデータ項目を保持するアプリケーションがＩＣカードにリストアされたとき、アプリケーションプログラムはＩＣカードのオペレーティングシステムからアプリケーションプログラムがＩＣカードの外部から読み込まれたアプリケーションプログラムであることを示す情報を受け取り、アプリケーションプログラムはその情報に基づいて予め定められたデータ項目に特定の値をセットすることを特徴とする。

また、本発明の一態様によるプログラムは、ＩＣカードに格納され、処理を行うプログラムであって、プログラムがＩＣカードに格納されたことを示す情報を得る手段及び該情報に基づいてＩＣカード内の所定領域に特定の値をセットする手段を実現することを特徴とする。ＩＣカード内の所定領域に特定の値をセットするとは、例えば電子マネーやポイント等のバリューをゼロにセットすることを意味する。この方法によると、バリューを扱うアプリケーションプログラムを外部からＩＣカードに格納する操作によってＩＣカード内に不正なバリューを生成することを禁止することができる。

本発明によると、ＩＣカードのメモリ内容を暗号機能を用いてＩＣカード外の装置にセキュリティ面で安全にバックアップし、自カードだけでなく別カードに対してもリストアすることが可能になる。

また、本発明の一態様によるＩＣカードにデータを格納する方法は、ＩＣカー

ドの外部に格納されたデータをＩＣカードに格納するとき、該データがＩＣカードの外部から読み込まれたことを認知するプログラムからその旨を示す情報を受け取り、その情報に基づいて予め定められた領域に該データの管理情報をセットすることを特徴とする。この方法は、ＩＣカードのメモリにデータ、例えば電子マネー等のバリューデータを書き込む領域と、そのバリューデータ書き込み履歴情報を格納する領域とをそれぞれ別個の領域として設定しておき、データの書き込み履歴等を管理するものである。

本発明の一態様によるＩＣカードにデータを格納する方法は、また、ＩＣカードの外部に格納されたデータをＩＣカードに格納するとき、該データがＩＣカードの外部から読み込まれたことを認知する回路からその旨を示す情報を受け取り、その情報に基づいて予め定められた領域に該データの管理情報をセットすることを特徴とする。この方法も、ＩＣカードのメモリにデータ、例えば電子マネー等のバリューデータを書き込む領域と、そのバリューデータ書き込み履歴情報を格納する領域とをそれぞれ別個の領域として設定しておき、データの書き込み履歴等を管理するものである。

本発明の一態様による、ＩＣカードに格納され、処理を行うプログラムは、データがＩＣカードに格納されたことを示す情報を得る手段及び該情報に基づいてＩＣカード内の所定領域に該データの管理情報をセットする手段を実現することを特徴とする。

図面の簡単な説明

第１図は、本発明によるＩＣカードとその内容をバックアップする外部装置の機能及び情報の流れの一例を示す全体構成図である。

第２図は、鍵の搬出機能と搬入機能の機能構成図である。

第３図は、差分バックアップ機能、リストア機能の機能構成図である。

第４図は、変更メモリ管理テーブルのデータ構造図である。

第５図は、保管データのデータ構造図である。

第６図は、カードＡＰ連携機能の機能構成図である。

第７図は、バックアップデータのデータ構造図である。

第８図は、バックアップデータを構成するレコードのデータ構造図である。

第９図は、別カードに対するリストアデータのデータ構造図である。

第１０図は、バックアップ対象メモリのデータ構造図である。

第１１図は、ＡＰ管理テーブルのデータ構造図である。

第１２図は、全体の実行手順のフローチャートである。

第１３図は、カードの初期化コマンド処理のフローチャートである。

第１４図は、バックアップコマンド処理のフローチャートである。

第１５図は、バックアップデータ転送コマンド処理のフローチャートである。

第１６図は、バックアップ完了コマンド処理のフローチャートである。

第１７図は、リストアコマンド処理のフローチャートである。

第１８図は、リストアデータ転送コマンド処理のフローチャートである。

第１９図は、リストア完了コマンド処理のフローチャートである。

第２０図は、カードＡＰのバリュー初期化処理のフローチャートである。

第２１図は、ＩＣカードとＩＣカード発行者の関係の例を示す模式図である。

発明を実施するための最良の形態

本発明をより詳細に説述するために、添付の図面に従ってこれを説明する。なお、以下の図には本発明の説明に当たって必要な機能のみを図示してあり、本発明の説明に直接必要のない機能については図示を省略してある。

ＩＣカードはＩＣチップを搭載しており、このＩＣカード用ＩＣチップは通常、ＣＰＵと３種類のメモリで構成されている。３種類のメモリは、書き換え不可能な不揮発メモリＲＯＭ（read only memory）、書き換え可能な不揮発メモリＥＥＰＲＯＭ（electrically erasable and programable read only memory）、及び書き換え可能な揮発メモリＲＡＭ（random access memory）である。また、ＩＣカードは通常ＩＣカードリーダ／ライタと呼ばれる装置を介して携帯端末、ＰＣ等の外部装置とコマンドおよびコマンド応答という方法で情報のやり取りをする。コマンドによってカードに渡すデータをコマンドデータといい、カードがコマンド処理結果として渡すコマンド応答としては、応答データと応答コードがある。ＩＣカードとＩＣカードリーダ／ライタの間における情報のやり取りの方式とし

ては、接触式のタイプ、非接触式のタイプ、接触式でも非接触式でも情報のやり取りができるハイブリッドタイプのものがあり、本発明はこれらいずれのタイプのＩＣカードに対しても適用できる。

第１図は、本発明によるＩＣカードとその内容をバックアップするコンピュータ等の外部装置の機能及び情報の流れの一例を示す全体構成図である。情報の流れは、暗号化されている情報を破線で、暗号化されていない情報を実線で示す。

ＩＣカード(001)内にはＥＥＰＲＯＭ(002)の内容をパーソナルコンピュータ(ＰＣ)などの外部装置(040)にバックアップするバックアップ機能(003)、外部装置からそのバックアップしたデータをリストアするリストア機能(004)、およびバックアップデータの暗号化と復号を行うための暗号機能(005)を備える。また、バックアップデータを暗号化と復号するためカード内だけに存在するカード固有の暗号鍵(008)を備える。このカード固有の暗号鍵はカード内で生成してもよいし、外部装置から安全に受取る手段を備えてもよい。但し、カード固有の暗号鍵(008)はカード内だけに保持することでバックアップデータの安全性をより高めることができる。このようにバツクアップされるデータは、カード内で暗号化されること、さらにカード内だけに復号できる手段を設けることで安全になる。すなわち、本発明によるＩＣカード(001)は、カード内にカード固有の暗号鍵(008)を保持するとともに、その暗号鍵(008)を用いて情報の暗号化処理(006)及び復号処理(007)を行う暗号機能(005)を備え、バックアップデータ(010)はカード固有の暗号鍵(008)で暗号化された状態で外部に取り出され、リストア時にはその暗号化された情報をカード内においてカード固有の暗号鍵(008)を用いて復号処理してリストアする。なお、リストア機能(004)は、プログラムではなく回路で実現することにより、処理の高速化を図ることができる。

また、バックアップデータを別のカードへリストアする場合、別カード内での復号が必要になる。このためカード固有の暗号鍵を別のカード（ＩＣカードｂ）へ渡す手段として鍵搬出機能(011)と鍵搬入機能(012)を備える。また、バックアップデータを外部装置上でディスク装置(043)などに保管する機能として保管機能(041)を、さらにその保管したバックアップデータを取出す機能として取出し機能(042)を備える。

第２図は、第１図に示したカード固有の暗号鍵(008)を別カードに渡す鍵搬出機能(011)と鍵搬入機能(012)の構成を示したものである。ＩＣカード内には、カード固有の暗号鍵(008)を別のカードへ暗号化して渡すためカード間で同一な共通暗号鍵(009)を備える。この共通暗号鍵の生成に関してはカード固有の暗号鍵と同様に、カード内で生成してもよいし、外部装置から安全に受取る手段を備えてもよい。また、カード内だけに保持することでバックアップデータの安全性をより高めることができる。カード固有の暗号鍵(008)は、バックアップ時に共通暗号鍵(009)で暗号化してバックアップデータ(010)の一部として外部装置に転送して保管する。また、リストア時は、外部装置(040)から転送されバックアップデータとして渡されるカード固有の暗号鍵を共通暗号鍵(009)で復号することでカード固有の暗号鍵(008)の受け渡しを実現する。さらにこの復号したカード固有の暗号鍵(008)を使用してバックアップデータ(010)を復号することにより別カード内でのリストアを実現する。

第３図は、変更されているメモリ内容だけをバックアップする差分バックアップ機能と差分リストア機能の構成を示す。ＩＣカード(001)内には、変更されているメモリ内容だけをバックアップしリストアする機能として差分バックアップ機能(020)と差分リストア機能(021)備える。差分バックアップでは、前回バックアップあるいはリストアした時点から変更されているメモリをチェックする手段として変更メモリ管理テーブル(022)をＥＥＰＲＯＭ(002)内のバックアップの対象としない場所に設ける。差分バックアップで変更されているメモリ内容だけをバックアップすることにより処理時間と格納媒体の容量削減を実現できる。

第４図に、変更メモリ管理テーブルのデータ構造を示す。第４図に示すとおり、変更メモリ管理テーブル(022)は、ＥＥＰＲＯＭ(002)を固定長（ページ）(090)単位ごとに分割し、ページごとに変更の有無を判断できるフラグ(091)を保持する。またこのフラグをセットする手段は、ハードウェアあるいはプログラムによって用意する。また、カードの初期化、バックアップ、およびリストアの実行後はフラグのリセットを行う。この差分バックアップは、全体バックアップと組み合わせて利用することにより効果が大きい。さらに、一つの全体バックアップと一連の複数の差分バックアップが外部装置側に保管されている場合、第５図に

示すバックアップデータの管理情報として格納されているバックアップ順序番号(061)とバックアップ種別(063)を元にこれらを順番に取出し順番にリストアする手段を外部装置(040)側に設けることによりリストアの効率的な実行を可能にする。

第５図は、外部装置上に保管されるバックアップデータのデータ構造を示す。外部装置上に保管するとき、バックアップデータの管理情報として、カード固有のカード番号(060)、バックアップ順序番号(061)、バックアップ日付(062)、バックアップ種別(063)等を生成あるいはカードから取得してバックアップデータと対応させて保管する。バックアップ順序番号(061)は、バックアップ実行ごとに順番に付けた番号である。バックアップ種別(063)は、全体バックアップと差分バックアップを識別するものである。

第６図は、ＡＰによるバリュー初期化手段を提供するカードＡＰ連携機能(032)の構成を示す。この図は、ＩＣカード(001)内のプログラムをＯＳ(030)とＡＰ(031)に別けて構成させ、このバックアップをＯＳ(030)の機能として実現する場合の例を示している。

電子マネー等のバリューを持つＡＰ(031)のリストアを実行すると、そのバリューがバックアップ時点に戻ってしまう不都合を回避する方法として、リストアを実行した場合、リストアを実行したことをＡＰごとに示すＡＰのリストア実行フラグ(086)をＯＳ内に設け、またそのフラグの状態をＡＰに通知する手段とＡＰがこのフラグをリセットする手段をＡＰに提供する機能としてカードＡＰ連携機能(032)を備える。電子マネーなどのバリューを持つＡＰは、保有するバリューを利用する前にリストアが実行されているかどうかをまずチェックし、リストアが実行されている場合バリューを初期化するなどの処置をした後、バリューに対する処理をする必要がある。また、ＡＰは一旦バリューの初期化を行った場合、リストア実行フラグ(086)のリセットをＯＳに要求する必要がある。

バックアップする機能をＯＳの機能として実現することにより、ＡＰに負担を強いることなくバックアップを実現できる。さらに、電子マネー、ポイント等のバリューを持つＡＰに対しては、リストアを実行後に該バリュー初期化できる手段を実現することでバックアップの適用範囲を拡大できる。

第７図は、外部装置に転送されるバックアップデータのデータ構造を示す。バックアップデータ(010)は、カード固有の暗号鍵(008)、バックアップ制御情報(050)、および実際のバックアップするメモリ内容であるデータ部(053)で構成させる。また、バックアップ制御情報(050)として、バックアップをしたカードのカード固有のカード番号(051)、全体バックアップと差分バックアップを識別するバックアップ種別(052)を持たせる。カード番号は、自カードにリストアするとき一致のチェックに利用する。このカード番号の一致チェックにより発生し易い作業ミスを防止できる。また、カード固有の暗号鍵(008)だけはカード共通暗号鍵(009)で暗号化し、これ以外はカード固有の暗号鍵(006)で暗号化する。またデータ部(053)は、複数のレコード(054)で構成させる。

第８図は、データ部(053)を構成するレコード(054)のデータ構造を示す。各レコードは、バックアップしたメモリ内容(056)とそのメモリ内容のＥＥＰＲＯＭ上の位置を示すフィールド(055)で構成する。また、各レコードは単一のページと複数のページのどちらで構成されていてもよい。

第９図は、別カードに対してリストアをする場合のリストアデータのデータ構造を示す。バックアップデータを別カードに対してリストアする場合、予め取得しておいたリストアするカードのカード番号(070)をバックアップデータ(010)に付加してカードに転送する。これによって、リストア時、この渡されたカード番号と実際にリストアをするカードの一致をチェックできる。このカード番号の一致チェックにより、発生し易い作業ミスを防止できる。

第１０図は、バックアップの対象となるＥＥＰＲＯＭ(002)のデータ構造を示す。この図は、ＩＣカード内のプログラムをＯＳとＡＰとに別けて構成させる例であり、この場合ＥＥＰＲＯＭはＯＳが利用するシステム領域(080)とＡＰのプログラムコード、データが格納されるＡＰ領域(081)で構成させる。システム領域(080)は、ＯＳ自身の領域とＯＳがＡＰを管理、実行するために用いるＡＰ管理テーブル(082)用の領域で構成させる。

第１１図は、ＡＰ管理テーブルのデータ構造を示す。ＡＰ管理テーブル(082)には、ＡＰごとに各ＡＰのＥＥＰＲＯＭ上の位置とサイズ(085)、および該ＡＰがリストアを実行したかどうかを示すフラグ(086)を設ける。ＥＥＰＲＯＭ上の

ＡＰの位置とサイズは、各ＡＰがリストアを実行したかどうかを判断するために利用する。

第１２図に、本発明によるバックアップとリストアの全体の実行手順のフローチャートを示す。ＩＣカードは通常、カード発行前にカードの初期化機能(105)によってカードの初期化が行われる。このカードの初期化ため、カードは初期化コマンド処理(100)を備えている。また、バックアップを実行するためにカードで処理するコマンドとして、バックアップコマンド(107)、バックアップデータ転送コマンド(108)、バックアップ完了コマンド(109)の３種類のコマンドを備える。バックアップコマンドは、バックアップの実行を要求するコマンドである。バックアップデータ転送コマンドは、バックアップデータを分割して転送するコマンドである。また、バックアップ完了コマンドは、外部装置上でのバックアップ処理が正常に完了したことをカードに通知するコマンドである。また、リストアを実行するためカードで処理するコマンドとして、リストアコマンド(110)、リストアデータ転送コマンド(111)、リストア完了コマンド(112)の３種類のコマンドを備える。リストアコマンドは、リストアの実行を要求するコマンドである。リストアデータ転送コマンドは、リストアするバックアップデータを分割して転送するコマンドである。また、リストア完了コマンドは、外部装置上のリストア処理が正常に完了したことをカードに通知するコマンドである。

次に、初期化コマンド処理の動作を第１３図のフローチャートにより説明する。カードは、カード初期化コマンド(106)を受け取ると、バックアップ用のカード固有の暗号鍵を生成し、ＥＥＰＲＯＭのシステム領域に格納する(120)。また、バックアップ用のカード共通暗号鍵を生成し、ＥＥＰＲＯＭのシステム領域に格納する(121)。また、次に本来のカードの初期化処理を実行し(122)、その後変更メモリ管理テーブルを初期化する(123)。

次に、バックアップコマンド処理の動作を第１４図のフローチャートにより説明する。カードは、バックアップコマンド(107)を受け取ると、必要に応じてＯＳが備えている認証機能を利用してバックアップコマンドのコマンド認証チェックによりコマンドの妥当性を確認する(130)。次に、バックアップ処理中のＥＥＰＲＯＭの更新を回避するためにバックアップ処理中フラグをセットする(131)。

次に、ＥＥＰＲＯＭのバックアップ位置を示すポインタを初期化する(132)。次に、バックアップデータの一部であるカード固有の暗号鍵とバックアップ制御情報をバッファに取出してそれぞれカード共通暗号鍵とカード固有の暗号鍵で暗号化する(133, 134, 135, 136)。この暗号化したデータをコマンド応答データとして送信する(137)。

次に、バックアップデータ転送コマンド処理の動作を第１５図のフローチャートにより説明する。カードは、バックアップデータ転送コマンド(108)を受け取ると、差分バックアップ要求かどうか判定し(140)、差分バックアップ要求でなければ、バックアップコマンド処理で設定したバックアップ開始ポインタからページ単位でデータをバッファに取出す(141)。また、差分バックアップ要求であれば、変更メモリ管理テーブル(022)を参照してバックアップ開始ポインタからページ単位で変更されているページのデータをバッファに取出す(142)。次に、バックアップ開始ポインタを次のページを取出すために更新する(143)。次に、バッファに取出したデータをカード固有の暗号鍵で暗号化する(144)。次に、暗号化したデータをコマンド応答データとして送信する(146)。また、対象となる全てのページのバックアップ処理が完了した場合、暗号化したデータの送信に合わせて、その旨をコマンド応答コードとして送信する(147)。

次に、バックアップ完了コマンド処理の動作を第１６図のフローチャートにより説明する。カードは、バックアップ完了コマンド(109)を受け取ると、変更メモリ管理テーブル(022)を初期化し(150)、バックアップ処理中フラグをリセットする(151)。また、処理結果をコマンド応答コードで送信する(152)。

次に、リストアコマンド処理の動作を第１７図のフローチャートにより説明する。カードは、リストアコマンド(110)を受け取ると、まずバックアップコマンド処理と同様にコマンドの認証チェックをする(160)。次に、リストア処理中のＥＥＰＲＯＭの更新を回避するためにリストア処理中フラグをセットする(161)。次に自カードへのリストアが要求されているかどうか判定し(162)、自カードへのリストアが要求されている場合、コマンドデータとして渡されたバックアップ制御情報をカード固有暗号鍵で復号し(163)、リストア処理に必要な情報を得る。この制御情報から得たカード番号とこのリストアを行っているカードのカード番

号の一致チェックをしてリストア処理の妥当性を確認する(164)。

また、バックアップをしたカードとは別なカードへのリストアが要求されている場合、まずコマンドデータとして渡されたリストア対象カードのカード番号とこのリストアを行っているカードのカード番号の一致チェックをしてリストアの妥当性を確認する(165)。次に、リストアデータとして渡されたバックアップしたカードのカード固有の暗号鍵をカード共通暗号鍵で復号する(166)。さらに、この復号した別カードのカード固有の暗号鍵をリストア処理で使用するように設定する(167)。次に、処理結果をコマンド応答コードとして送信する(168)。

次に、リストアデータ転送コマンド処理の動作を第１８図のフローチャートにより説明する。カードは、リストアデータ転送コマンド(111)を受け取ると、コマンドデータとしてバッファに読み込まれたバックアップデータを、自カードへのリストアであれば自カードのカード固有暗号鍵で、また別カードへのリストアであれば渡された別カードのカード固有の暗号鍵で復号する(170)。復号したデータは、データに付加されているバックアップ位置にページ単位でデータを書き込む(171)。次に、差分リストア要求であれば、ＡＰ管理テーブルを参照してＡＰの位置とサイズからリストアしたページが属するＡＰのリストア実行フラグをセットする(174)。次に、処理結果をコマンド応答コードとして送信する(175)。

次に、リストア完了コマンド処理の動作を第１９図のフローチャートにより説明する。カードは、リストア完了コマンド(112)を受け取ると、差分リストア要求でなければ、全ＡＰのリストア実行フラグをセットする(181)。次に、変更メモリ管理テーブルを初期化し(182)、リストア処理中フラグをリセットする(183)。また、処理結果をコマンド応答コードで送信する(184)。差分リストア要求の場合には、変更メモリ管理テーブルを初期化し(182)、リストア処理中フラグをリセットし(183)、処理結果をコマンド応答コードで送信する(184)。

次に、ＡＰのバリュー初期化処理を第２０図のフローチャートにより説明する。ＡＰは、該ＡＰに対するコマンドを受取ると、通常まずＡＰが備えている認証機能を利用してコマンド認証チェックによりコマンドの妥当性を確認する(190)。次に、ＯＳが提供するカードＡＰ連携機能を利用して該ＡＰに対してリストアが実行されているかどうかのチェックをする(191)。リストアが実行されていれば、

該ＡＰが保持する電子マネー、ポイント等のバリューを初期化し(193)、さらにＡＰ連携機能を利用して該ＡＰに対するリストア実行フラグをリセットする(194)。この後、通常のコマンド処理を実行し(195)、処理結果を送信する(196)。ＯＳが提供するカードＡＰ連携機能を利用して該ＡＰに対してリストアが実行されているかどうかのチェックをし(191)、リストアが実行されていなければ通常のコマンド処理を実行し(195)、処理結果を送信する(196)。

また、第２０図では説明していないが、ＡＰのバリューを初期化する別の方法として、リストアが実行されていることをコマンド応答コードで一旦要求元に知らせ、要求元からＡＰのバリューを設定するコマンドを再発行させるという方法もある。また、これも図では説明していないが、ＡＰがバリューの初期化ルーチンをＯＳに登録しておき、リストアが実行された場合、次にＡＰが実行されるときその登録しておいた初期化ルーチンを実行して初期化処理を実行させるという方法もある。

第２１図は、ＩＣカードと、その中に格納されているアプリケーション、ＩＣカード発行者の関係の例を示す模式図である。この例に示すＩＣカード(001)にはアプリケーションとして、電子マネー(201)、クレジット(202)、身分証明書(203)、医療サービス(204)、会員サービス(205)等に関係する複数のアプリケーションが格納されている。ＩＣカード発行者は、そのサービスの一つとしてＩＣカードのメモリ内容のバックアップサービスを行う。カード発行者のホストコンピュータ(210)には、ＩＣカードのバックアップを取り、それをＩＣカードにリストアするサービスを行うためのプログラム(211,213)及びバックアップ用のデータベース(212)が格納されている。

ＩＣカード(001)のメモリ内容のバックアップは、ＩＣカード所有者がカード発行者の端末に所有のＩＣカードを読み取らせて定期的あるいは不定期に行ったり、アプリケーションのサービス提供者の端末とカード発行者のホストコンピュータ(210)とを通信網で接続しておき、ＩＣカード所有者がＩＣカードを使用したときサービス提供者の端末からカード発行者のホストコンピュータ(210)にバックアップデータを送信することで実行することができる。ＩＣカード所有者が自分が所有しているＩＣカードを紛失したときは、所定の手続をもってカー

ド発行者に申し出る。すると、カード発行者はバックアップ用のデータベース(212)に保管されているそのＩＣカードのバックアップデータを用いて新しいＩＣカード(214)を発行するサービスを行う。

以上、ＩＣカードのバックアップ方法及びリストア方法について詳細に説明してきたが、本発明は、これまで説明したＩＣカード内のＯＳやＡＰの機能あるいはＩＣカードに組み込まれた回路を用いて、ＩＣカードに外部からデータが格納されたとき、それを検知してＩＣカードの予め定められた領域にそのデータの格納日付や格納回数等のデータ管理情報を書き込むように拡張することができる。この方法は、例えば、ＩＣカードに電子マネーを取り扱うＡＰがロードされていてＩＣカードの外部から電子マネーが格納されたとき、電子マネーの書き込み領域とは別の領域にその電子マネー書き込み履歴情報を格納することを可能にするもので、電子マネーの書き込み履歴の管理に利用することができる。

産業上の利用可能性

以上のように、本発明のＩＣカード及びＩＣカードのバックアップ・リストア方法によれば、カード内だけに存在するカード固有の暗号鍵を用いて暗号化してバックアップし、またバックアップしたデータは同じＩＣカード内だけで復号してリストアすることにより、安全なバックアップを実現できる。また、カード内だけに存在するカード間で同一な共通暗号鍵を用いてカード固有の暗号鍵を暗号化して別カードに渡すことにより、別カードに対しても安全なリストアを実現できる。

請 求 の 範 囲

1．暗号鍵と、暗号化処理及び復号処理を行う暗号機能と、前記暗号鍵を用いて前記暗号機能の暗号化処理でＩＣカードのメモリに格納されている情報を暗号化したバックアップデータを搬出するバックアップ機能と、搬入した暗号化されたバックアップデータを前記暗号鍵を用いて前記暗号機能の復号処理で復号しメモリにリストアするリストア機能とを備えることを特徴とするＩＣカード。

2．当該ＩＣカードに固有の暗号鍵と、複数のＩＣカードに共通の暗号鍵と、暗号化処理及び復号処理を行う暗号機能と、前記固有の暗号鍵を用いて前記暗号機能の暗号化処理でＩＣカードのメモリに格納されている情報を暗号化したバックアップデータと前記共通の暗号鍵を用いて前記暗号機能の暗号化処理で暗号化した前記固有の暗号鍵とを含む情報を搬出するバックアップ機能とを備えることを特徴とするＩＣカード。

3．第１の暗号鍵と、暗号鍵を用いて復号処理を行う暗号機能と、搬入した暗号化された情報から前記第１の暗号鍵を用いて前記暗号機能の復号処理で第２の暗号鍵を復号する機能と、前記搬入した暗号化された情報から前記第２の暗号鍵を用いて前記暗号機能の復号処理でバックアップデータを復号しメモリにリストアするリストア機能とを備えることを特徴とするＩＣカード。

4．ＩＣカードに固有の暗号鍵と、複数のＩＣカードに共通の暗号鍵と、暗号化処理及び復号処理を行う暗号機能と、前記ＩＣカードに固有の暗号鍵を用いて前記暗号機能の暗号化処理でＩＣカードのメモリに格納されている情報を暗号化したバックアップデータと前記共通の暗号鍵を用いて前記暗号機能の暗号化処理で暗号化した前記ＩＣカードに固有の暗号鍵とを含む情報を搬出するバックアップ機能と、搬入した暗号化された情報から前記共通の暗号鍵を用いて前記暗号機能の復号処理でＩＣカードに固有の暗号鍵を復号する機能と、復号した前記ＩＣカードに固有の暗号鍵を用いて前記暗号機能の復号処理で復号したバックアップデータをメモリにリストアするリストア機能とを備えることを特徴とするＩＣカード。

5．請求項１記載のＩＣカードにおいて、前記バックアップデータにはＩＣカー

ドを識別する識別情報が含まれていることを特徴とするＩＣカード。

６．請求項１記載のＩＣカードにおいて、リストアを実行したことを示す情報を保持し、前記情報をカードアプリケーションに通知する機能を有するオペレーティングシステムを備えることを特徴とするＩＣカード。

７．請求項６記載のＩＣカードにおいて、前記アプリケーションは値そのものが経済的価値を有するデータ（バリュー）を扱うアプリケーションであり、当該アプリケーションは前記リストアを実行したことを示す情報を受け取ったとき前記バリューを初期化する処理を行うことを特徴とするＩＣカード。

８．当該ＩＣカードに固有の暗号鍵と、複数のＩＣカードに共通の暗号鍵と、暗号化処理及び復号処理を行う暗号機能と、前記共通の暗号鍵を用いて前記暗号機能の暗号化処理で暗号化した前記固有の暗号鍵を搬出する鍵搬出機能と、搬入した情報から前記共通の暗号鍵を用いて前記暗号機能の復号処理でＩＣカードに固有の暗号鍵を復号する鍵搬入機能とを備えることを特徴とするＩＣカード。

９．ＩＣカードのメモリ内容を前記ＩＣカード外の装置にバックアップするＩＣカードのバックアップ方法において、

前記メモリ内容を前記ＩＣカード内だけに存在する前記ＩＣカードに固有の暗号鍵を用い暗号化してバックアップデータとして前記ＩＣカード外の装置に搬出することを特徴とするＩＣカードのバックアップ方法。

１０．外部装置にバックアップしたＩＣカードのメモリ内容を前記ＩＣカードにリストアするＩＣカードのメモリ内容リストア方法において、

前記外部装置から搬入した暗号化されたバックアップデータを前記ＩＣカード内だけに存在する前記ＩＣカードに固有の暗号鍵を用い復号してメモリにリストアすることを特徴とするＩＣカードのメモリ内容リストア方法。

１１．請求項１０記載のＩＣカードのメモリ内容リストア方法において、前記バックアップデータはＩＣカードを識別する識別情報を含み、リストア時に前記バックアップデータに含まれている識別情報とリストアするＩＣカードの識別情報の一致をチェックすることを特徴とするＩＣカードのメモリ内容リストア方法。

１２．第１のＩＣカードのメモリ内容を外部装置にバックアップし、前記バックアップしたメモリ内容を第２のＩＣカードのメモリにリストアする方法において、

前記第１のＩＣカード内だけに存在する前記第１のＩＣカードの固有の暗号鍵を前記第１のＩＣカード内で前記第１および第２のＩＣカードに共通の暗号鍵を用いて暗号化したデータと、前記第１のＩＣカードのメモリ内容を前記第１のＩＣカードに固有の暗号鍵を用いて前記第１のＩＣカード内で暗号化したデータとを含むバックアップデータを前記第１のＩＣカードから前記外部装置に搬出するステップと、

前記第２のＩＣカードで前記外部装置から前記バックアップデータを搬入するステップと、

搬入した前記バックアップデータから、ＩＣカード内だけに存在する前記共通の暗号鍵を用いて、前記第２のＩＣカード内で前記第１のＩＣカードに固有の暗号鍵を復号するステップと、

搬入した前記バックアップデータから、復号した前記第１のＩＣカードに固有の暗号鍵を用いて、前記第２のＩＣカード内で前記第１のＩＣカードのメモリ内容を復号するステップと、

復号した前記第１のＩＣカードのメモリ内容を前記第２のＩＣカードのメモリにリストアするステップとを含むことを特徴とする方法。

１３．請求項１２記載の方法において、前記第１のＩＣカードのメモリ内容をリストアすべきＩＣカードの識別情報を予め取得してバックアップデータに付加しておき、バックアップデータに付加された識別情報と前記第２のＩＣカードが保持している識別情報の一致をチェックすることを特徴とする方法。

１４．ＩＣカードのメモリ内容を外部装置にバックアップし、バックアップしたメモリ内容をＩＣカードのメモリにリストアする方法において、

バックアップ対象メモリの内容変更の有無をメモリの分割単位（ページ）ごとに判断し、変更されているページだけのバックアップとリストアをすることを特徴とする方法。

１５．請求項１４記載の方法において、前記外部装置は、バックアップデータの管理情報としてバックアップの順序番号と当該バックアップが全体バックアップか変更ページだけの部分バックアップかの情報を保管しておき、この管理情報を用いて一連のバックアップデータを一括してリストアすることを特徴とする方法。

１６．ＩＣカードのメモリ内容を外部装置にバックアップし、バックアップしたメモリ内容をＩＣカードのメモリにリストアする方法において、

ＩＣカード内のプログラムをオペレーティングシステムとアプリケーションプログラムとに別けて構成し、バックアップ機能及びリストア機能をオペレーティングシステムの機能として実現することを特徴とする方法。

１７．請求項１６記載の方法において、アプリケーションプログラムは電子マネー、ポイント等のバリューを持ち、オペレーティングシステムがバックアップとリストアを実行した場合、オペレーティングシステムがアプリケーションプログラムにリストアの実行を通知し、リストアの実行を通知されたアプリケーションプログラムはバリューの利用前に当該バリューを初期化することを特徴とする方法。

１８．ＩＣカードにプログラムを格納する方法であって、前記ＩＣカードの外部に格納されたプログラムを前記ＩＣカードに格納するとき、該プログラムが前記ＩＣカードの外部から読み込まれたことを認知するプログラムからその旨を示す情報を受け取り、前記情報に基づいて前記ＩＣカード内の予め定められた領域に特定の値をセットすることを特徴とするＩＣカードにプログラムを格納する方法。

１９．ＩＣカードにプログラムを格納する方法であって、前記ＩＣカードの外部に格納されたプログラムを前記ＩＣカードに格納するとき、該プログラムが前記ＩＣカードの外部から読み込まれたことを認知する回路からその旨を示す情報を受け取り、前記情報に基づいて前記ＩＣカード内の予め定められた領域に特定の値をセットすることを特徴とするＩＣカードにプログラムを格納する方法。

２０．ＩＣカードに格納され、処理を行うプログラムであって、プログラムが前記ＩＣカードに格納されたことを示す情報を得る手段及び該情報に基づいて前記ＩＣカード内の所定領域に特定の値をセットする手段を実現することを特徴とするプログラム。

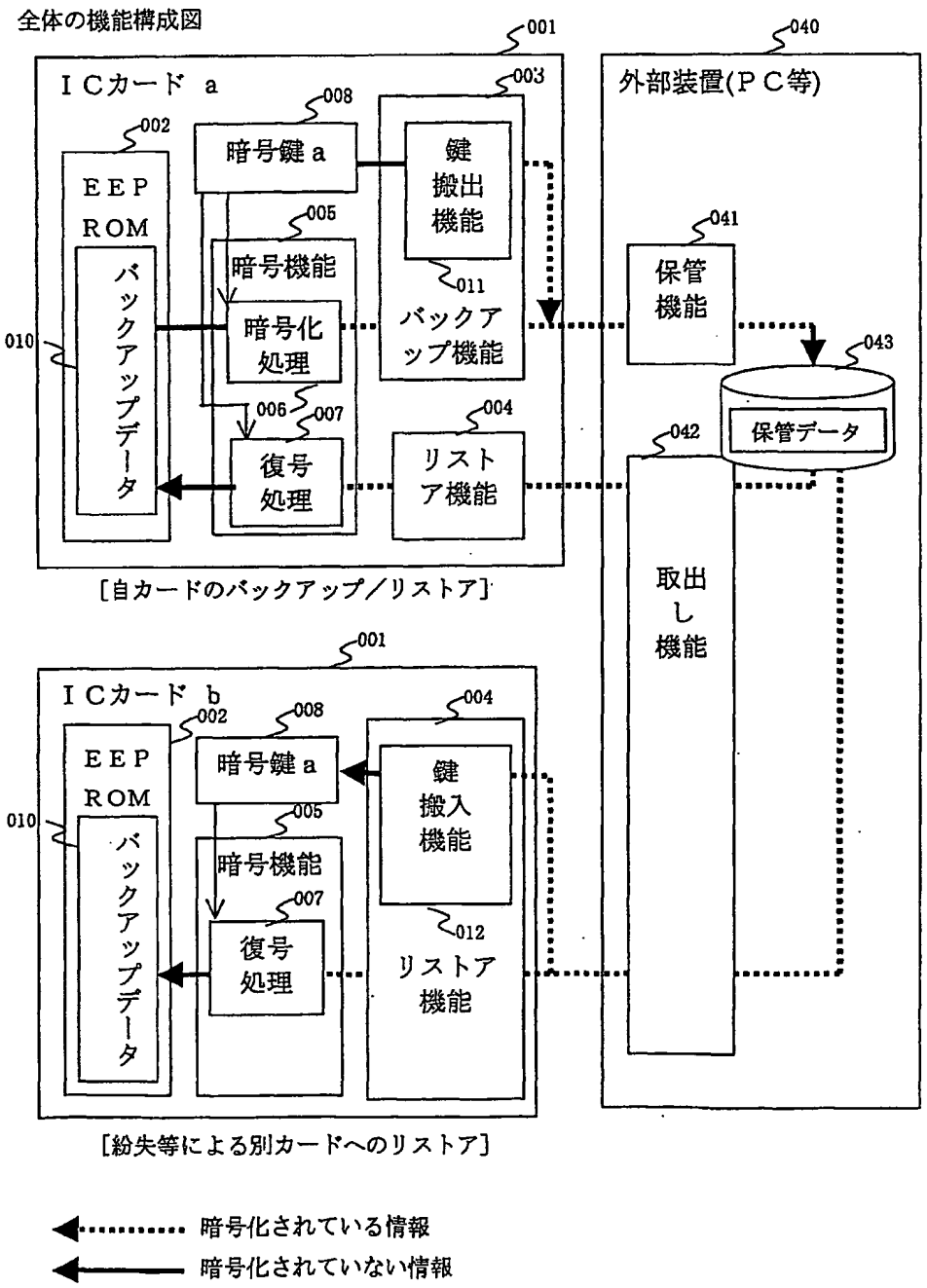
２１．ＩＣカードにデータを格納する方法であって、前記ＩＣカードの外部に格納されたデータを前記ＩＣカードに格納するとき、該データが前記ＩＣカードの外部から読み込まれたことを認知するプログラムからその旨を示す情報を受け取り、前記情報に基づいて予め定められた領域に該データの管理情報をセットする

ことを特徴とするＩＣカードにデータを格納する方法。

２２．ＩＣカードにデータを格納する方法であって、前記ＩＣカードの外部に格納されたデータを前記ＩＣカードに格納するとき、該データが前記ＩＣカードの外部から読み込まれたことを認知する回路からその旨を示す情報を受け取り、前記情報に基づいて予め定められた領域に該データの管理情報をセットすることを特徴とするＩＣカードにデータを格納する方法。

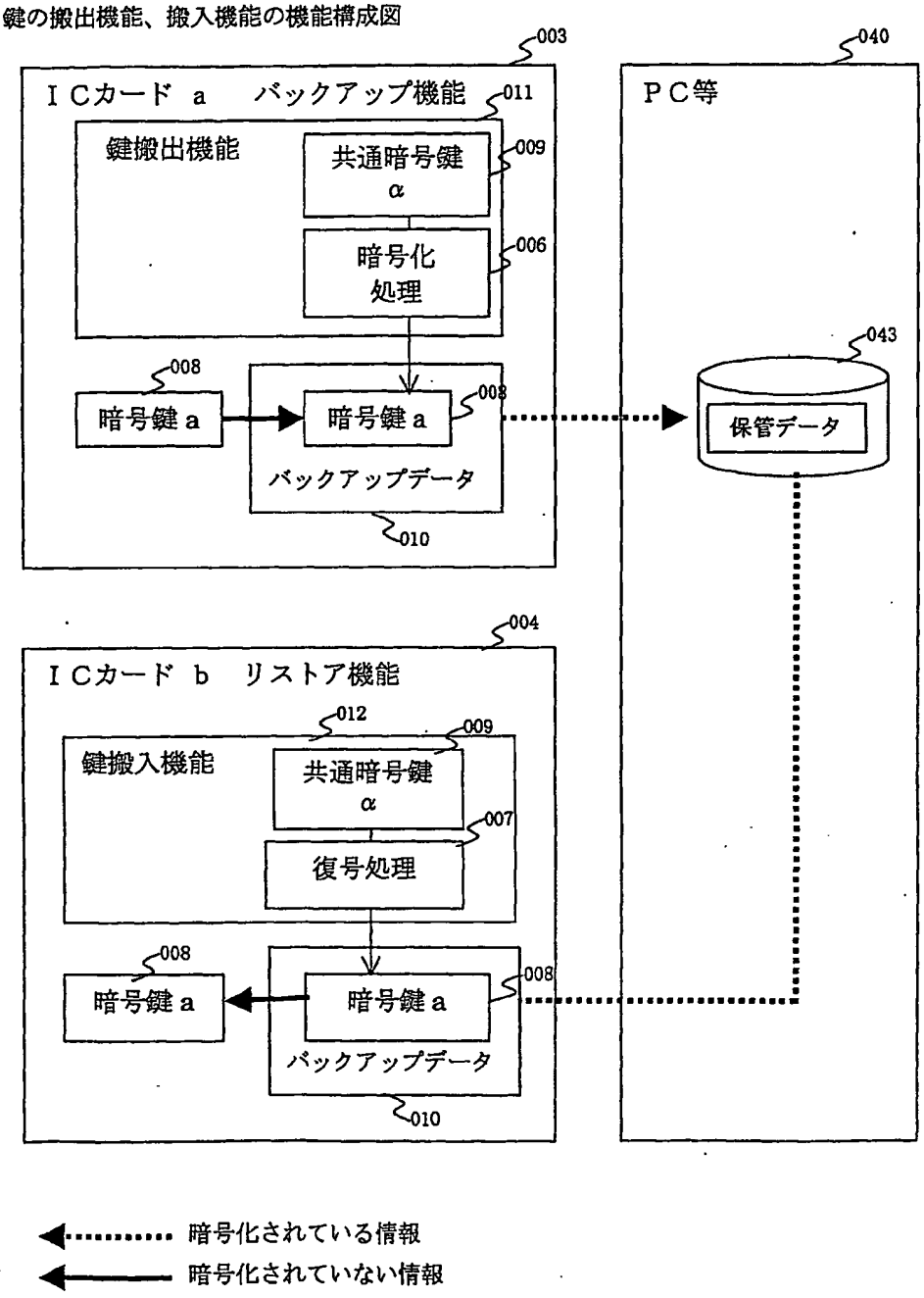
２３．ＩＣカードに格納され、処理を行うプログラムであって、データが前記ＩＣカードに格納されたことを示す情報を得る手段及び該情報に基づいて前記ＩＣカード内の所定領域に該データの管理情報をセットする手段を実現することを特徴とするプログラム。

第１図


全体の機能構成図
ＩＣカード a
001
003
008
002
暗号鍵 a
鍵
搬出
機能
ＥＥＰ
ＲＯＭ
005
暗号機能
011
バックア
ップ機能
010
バックアップデータ
暗号化
処理
006
007
004
復号
処理
リスト
ア機能
[自カードのバックアップ／リストア]
001
ＩＣカード b
002
008
004
ＥＥＰ
ＲＯＭ
暗号鍵 a
鍵
搬入
機能
010
005
暗号機能
007
012
復号
処理
リストア
機能
バックアップデータ
[紛失等による別カードへのリストア]
040
外部装置(ＰＣ等)
041
保管
機能
043
保管データ
042
取出
し
機能
暗号化されている情報
暗号化されていない情報

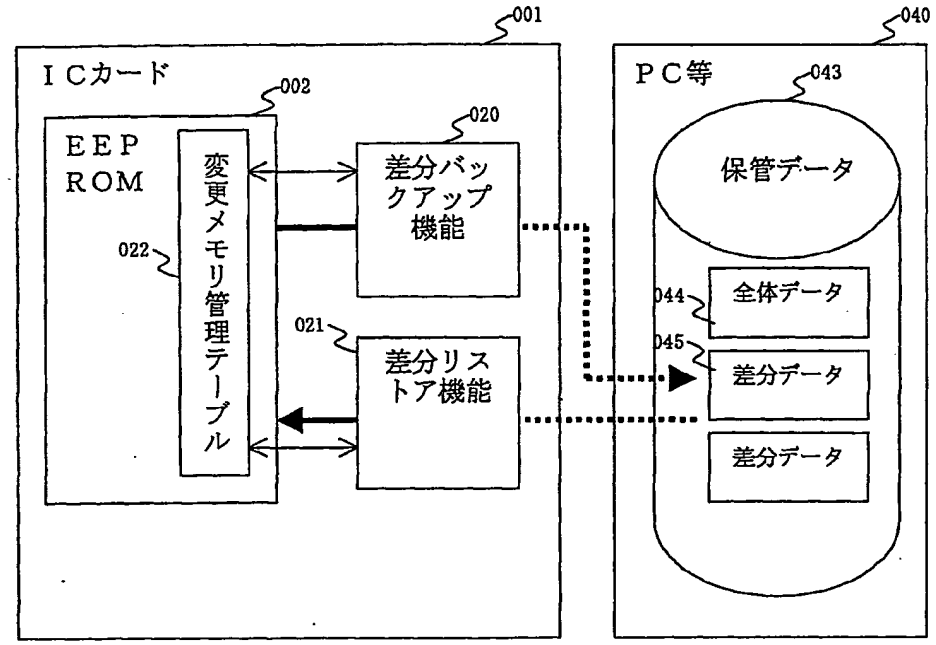
第２図

鍵の搬出機能、搬入機能の機能構成図



第３図

差分バックアップ機能，リストア機能の機能構成図

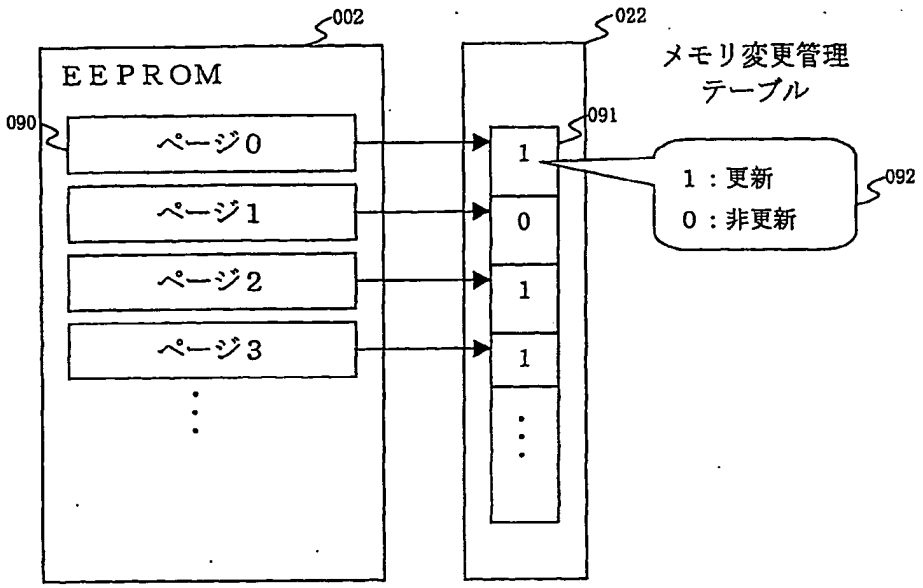


暗号化されている情報

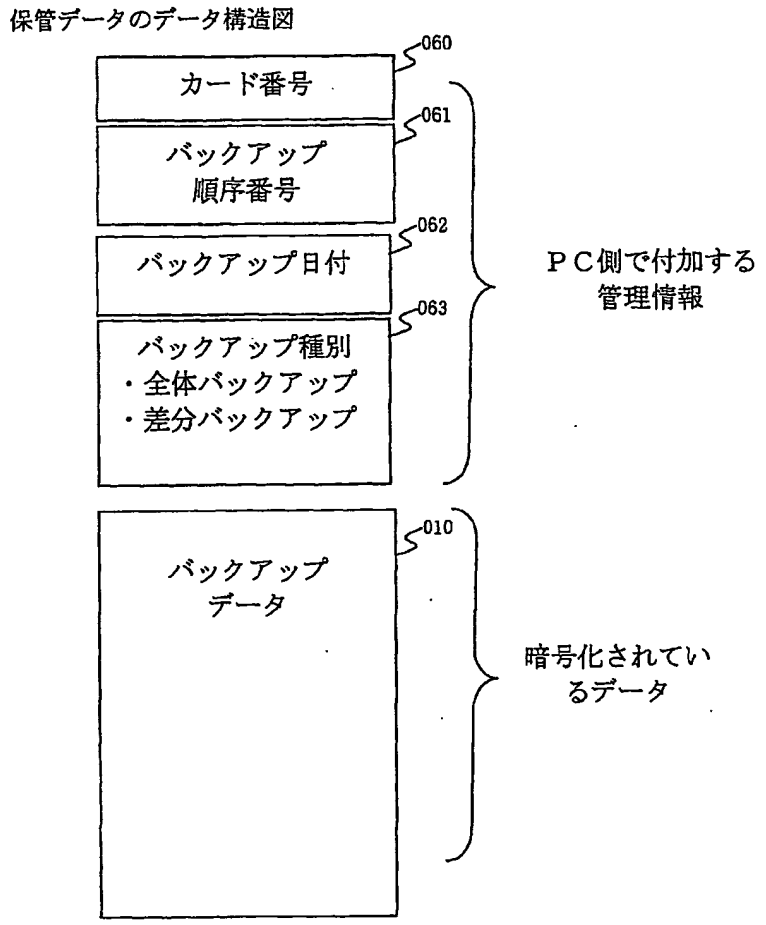
暗号化されていない情報

第４図

変更メモリ管理テーブルのデータ構造図

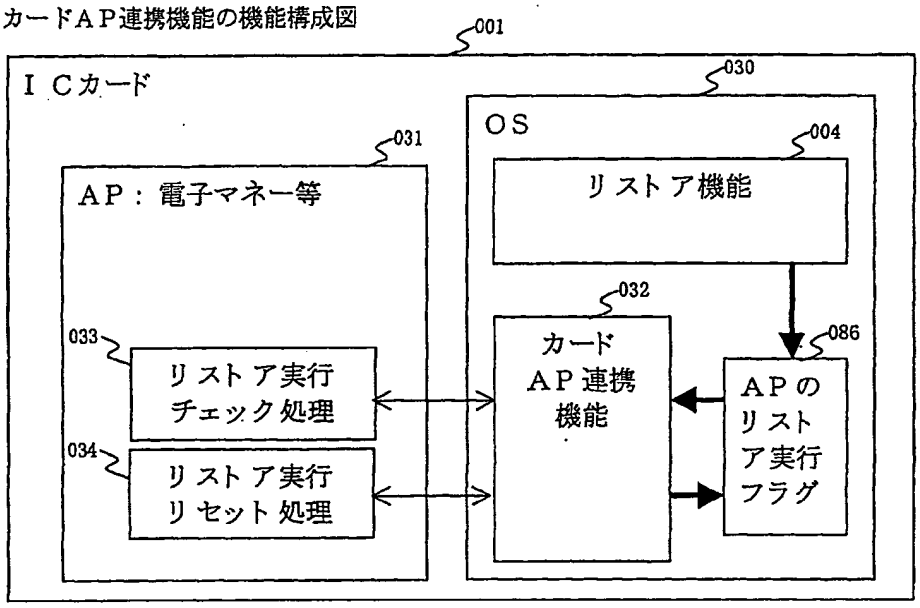


第５図


保管データのデータ構造図
060
カード番号
061
バックアップ
順序番号
062
バックアップ日付
063
バックアップ種別
・全体バックアップ
・差分バックアップ
ＰＣ側で付加する
管理情報
010
バックアップ
データ
暗号化されてい
るデータ

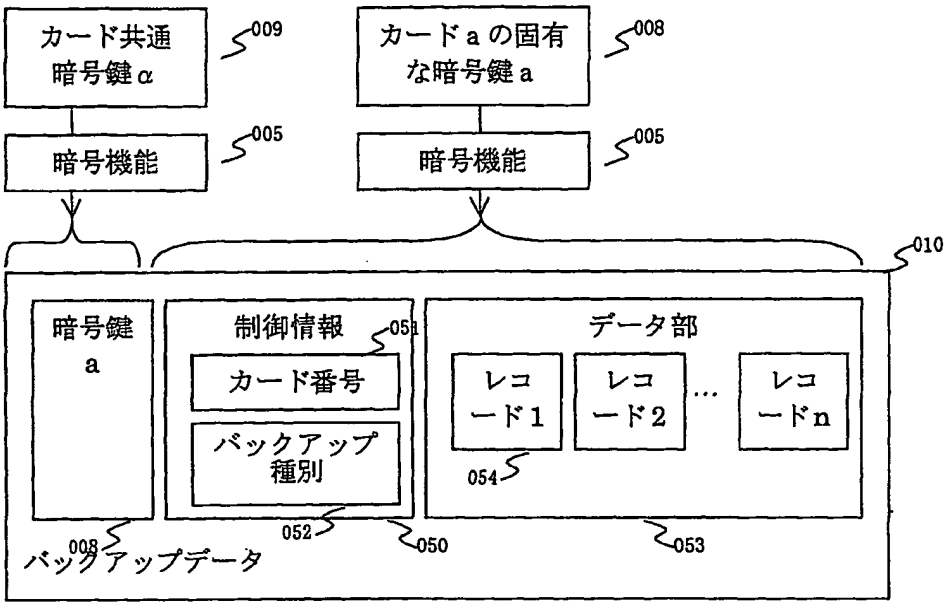
第６図

カードＡＰ連携機能の機能構成図



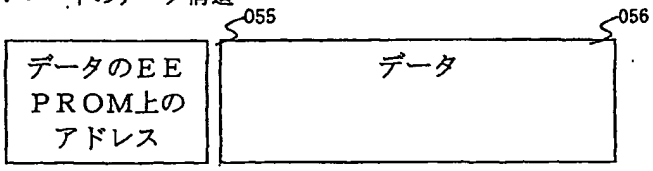
第７図

バックアップデータのデータ構造図



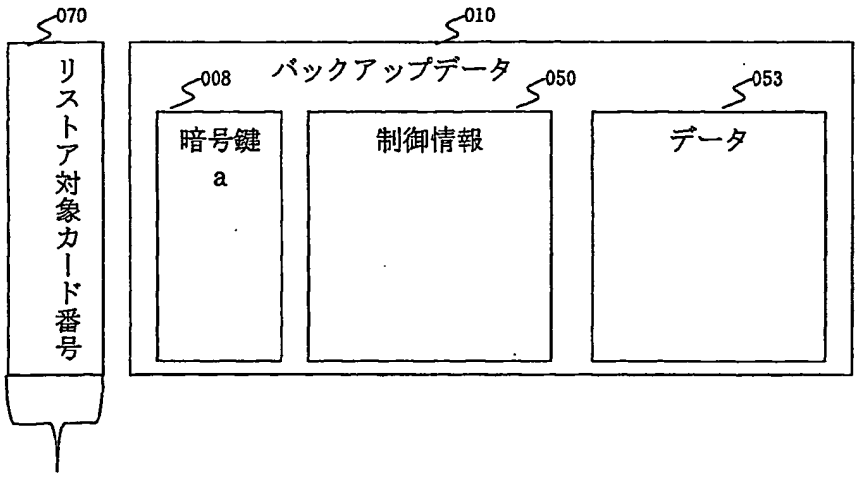
第８図

レコードのデータ構造



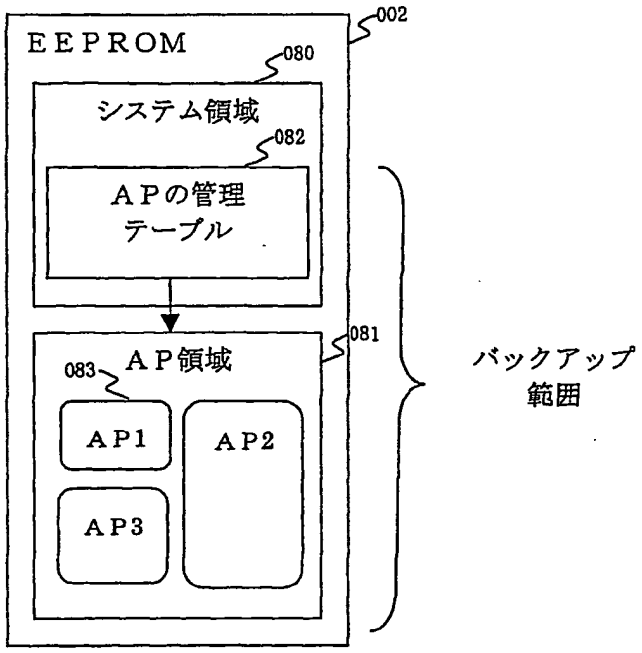
第９図

別カードへのリストアデータのデータ構造図



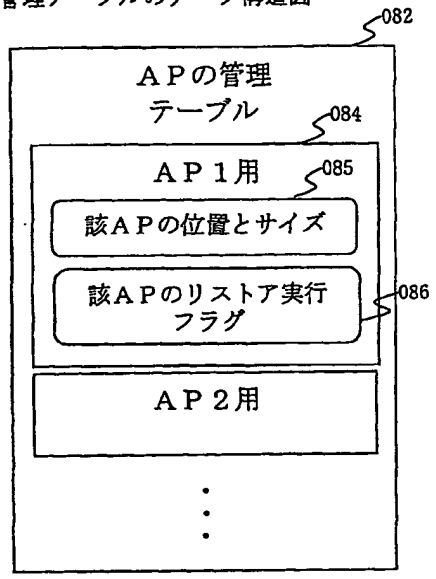
第１０図

バックアップ対象メモリのデータ構造図



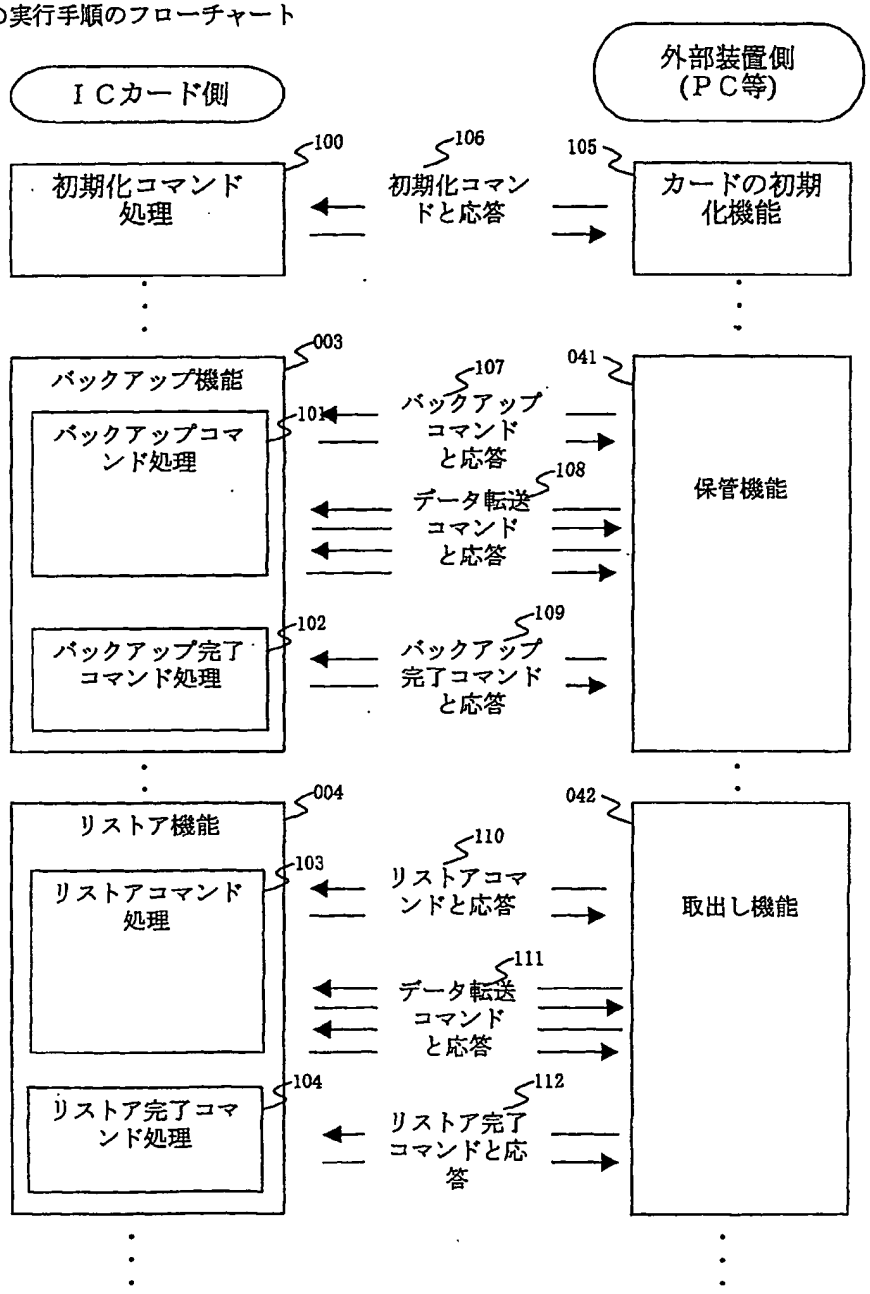
第１１図

ＡＰ管理テーブルのデータ構造図



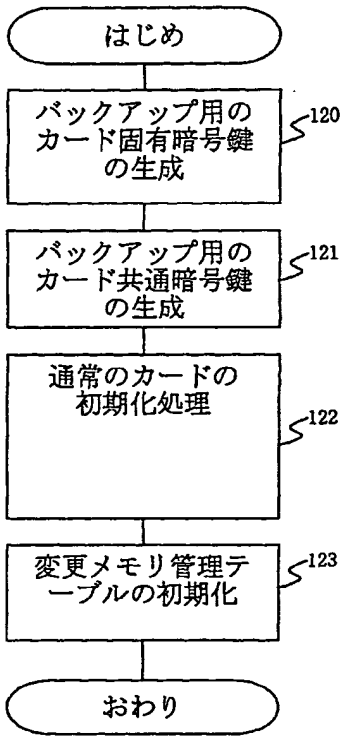
第１２図

全体の実行手順のフローチャート



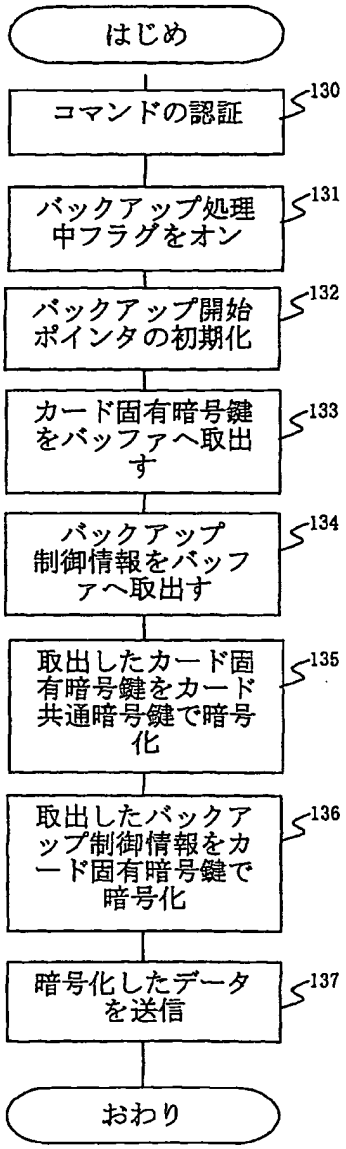
第１３図

初期化コマンド処理のフローチャート



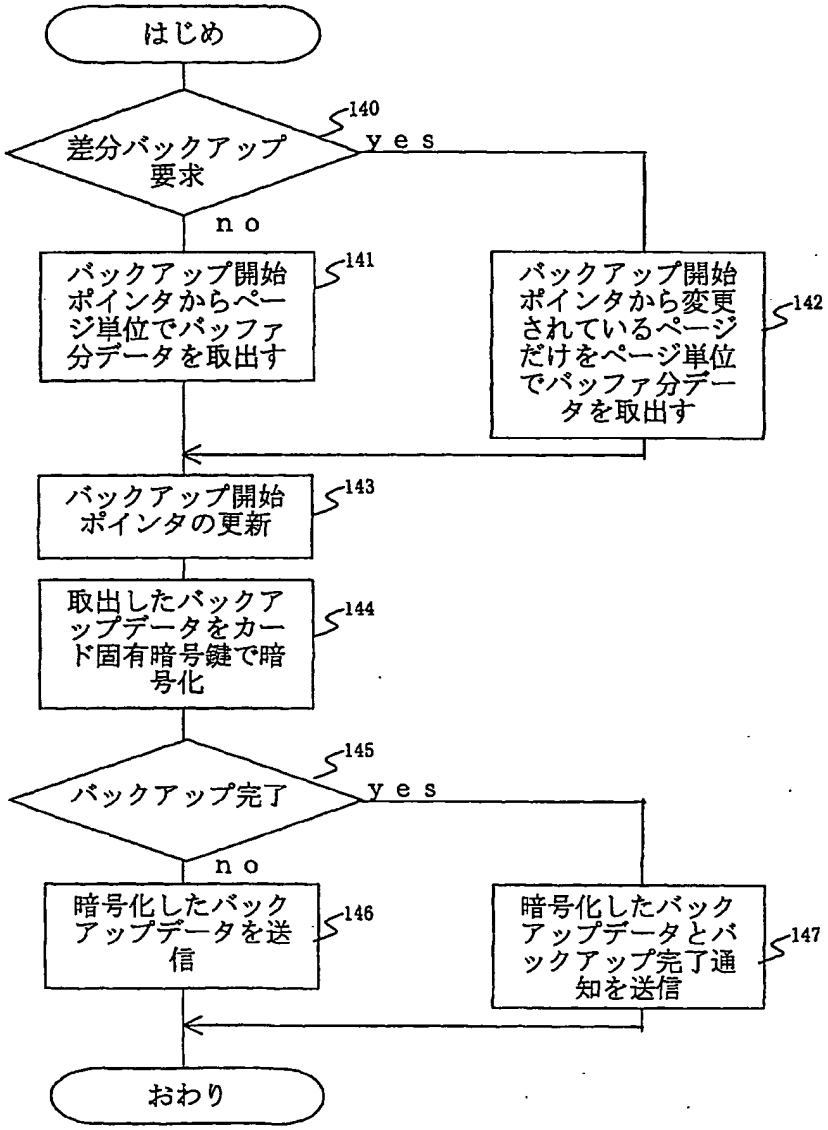
第１４図

バックアップコマンド処理のフローチャート



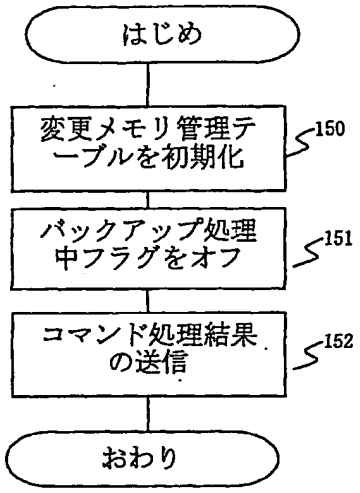
第１５図

バックアップデータ転送コマンド処理のフローチャート



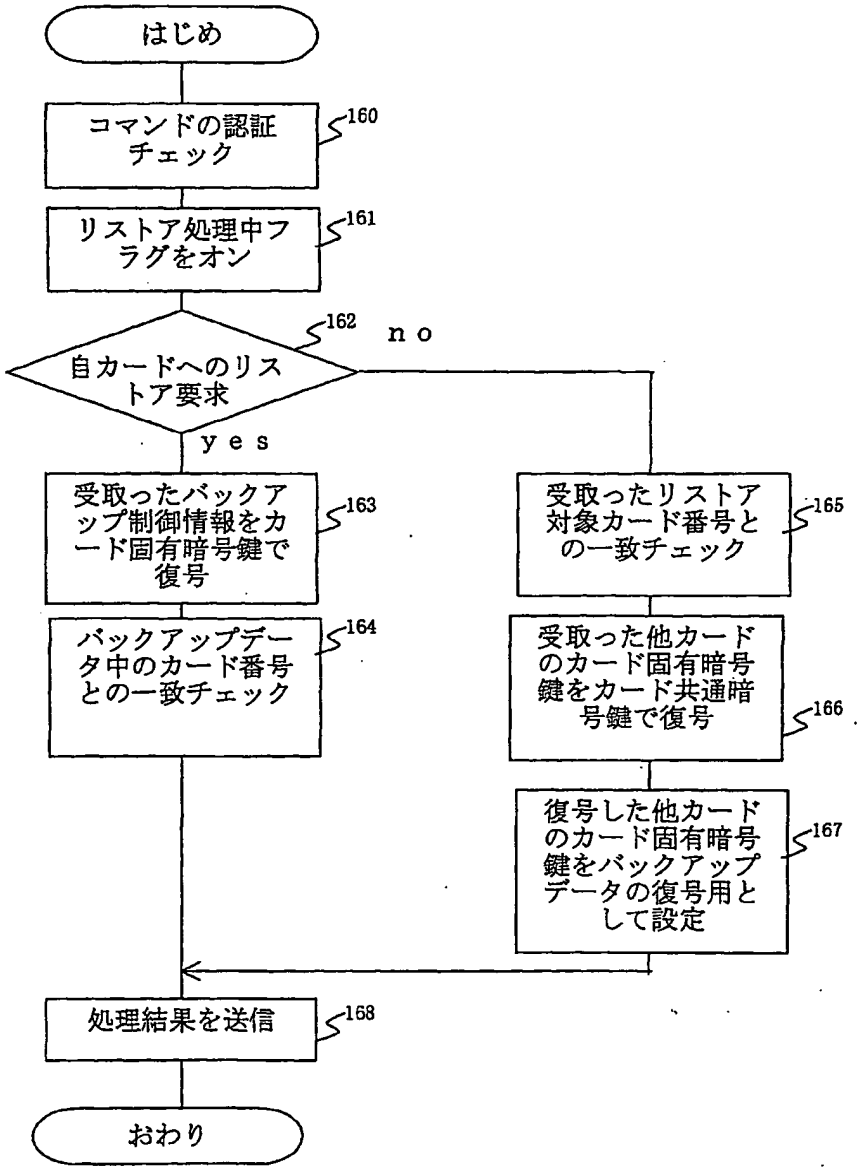
第１６図

バックアップ完了コマンド処理のフローチャート



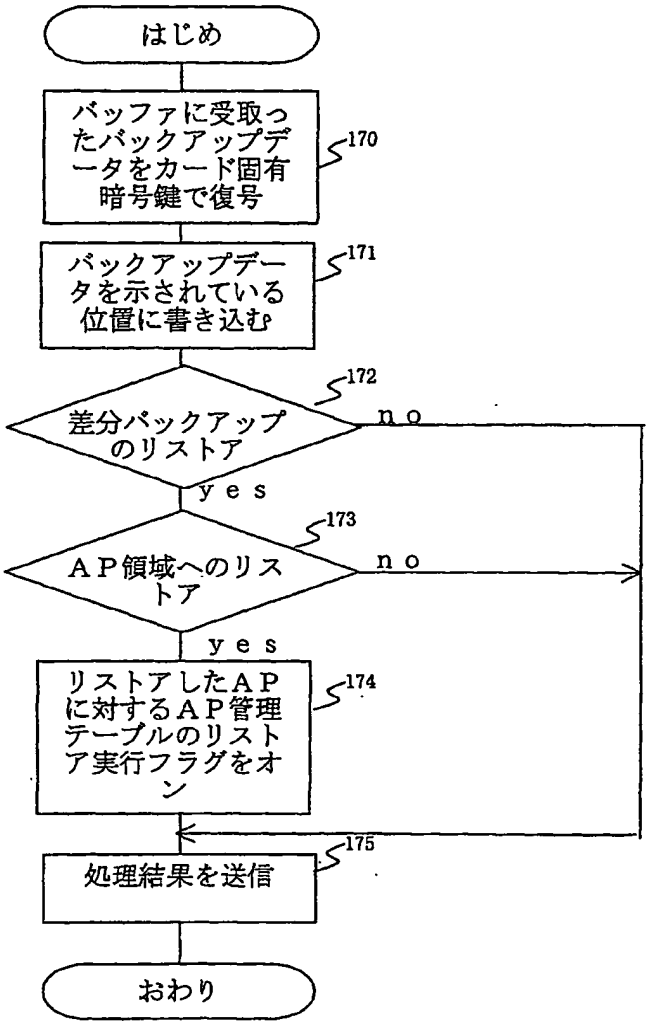
第１７図

リストアコマンド処理のフローチャート



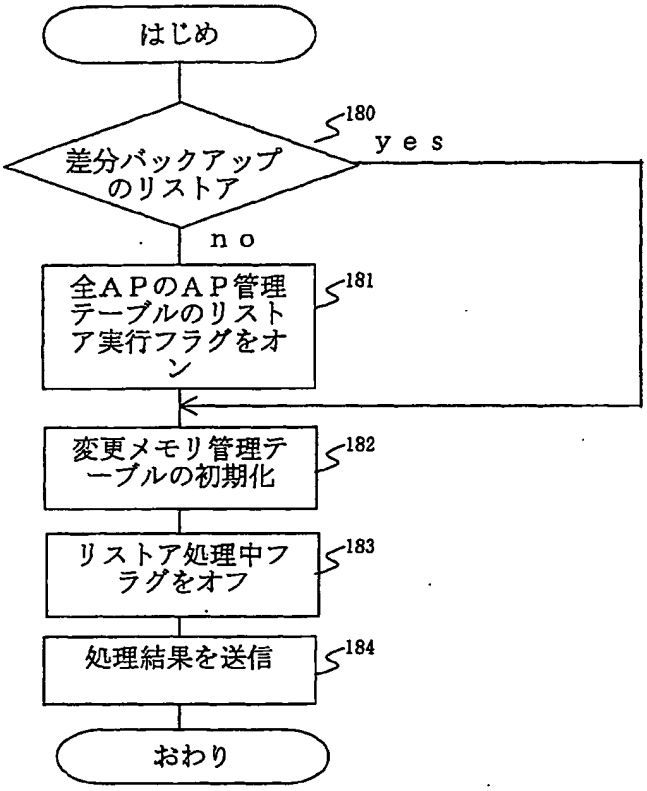
第１８図

リストアデータ転送コマンド処理のフローチャート



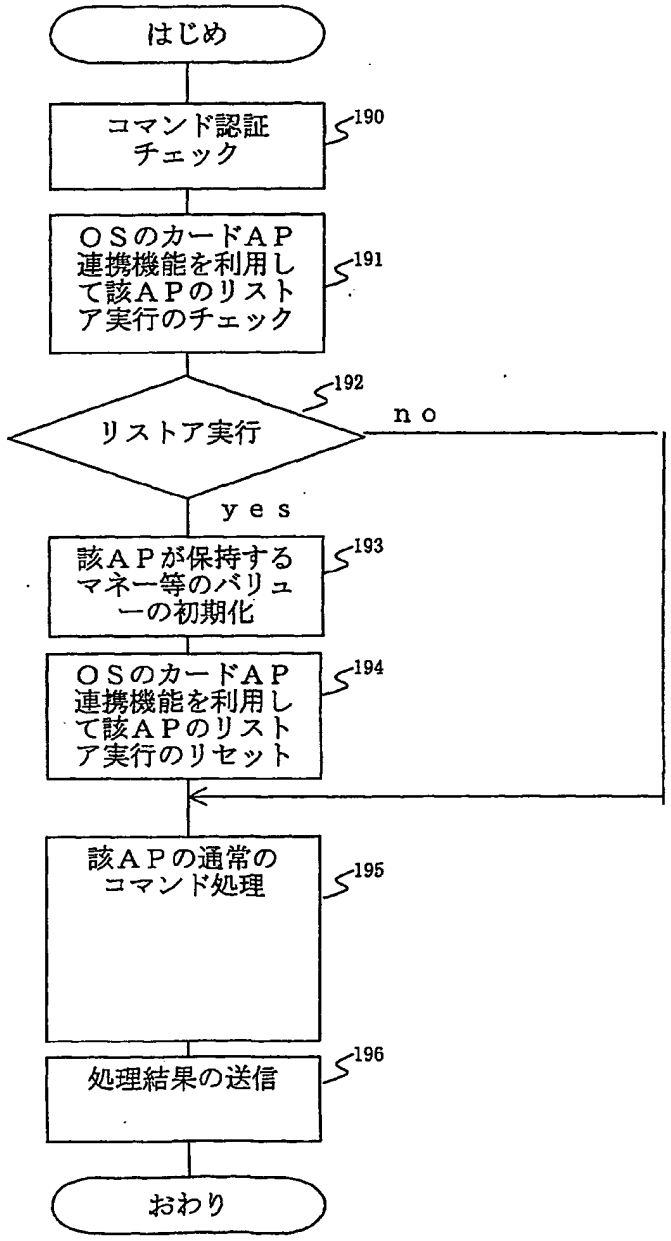
第１９図

リストア完了コマンド処理のフローチャート

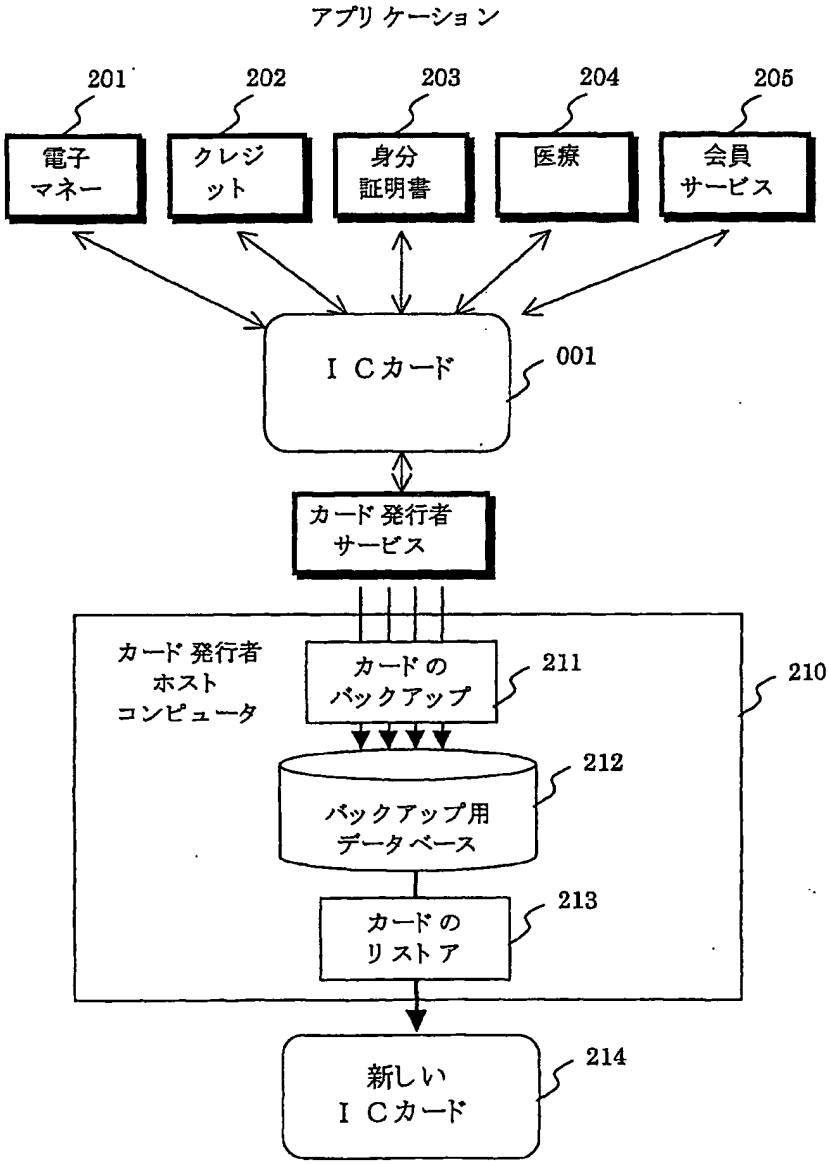


第２０図

カードＡＰのバリュー初期化処理のフローチャート



第２１図


アプリケーション
201
202
203
204
205
電子マネー
クレジット
身分証明書
医療
会員サービス
ＩＣカード
001
カード発行者サービス
カード発行者ホストコンピュータ
カードのバックアップ
211
210
212
バックアップ用データベース
213
カードのリストア
新しいＩＣカード
214

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/04447

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F17/60, G06K19/07

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F12/00, G06F12/16, G06F17/60,
G06K17/00, G06K19/07-19/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2000
Kokai Jitsuyo Shinan Koho 1971-2000 Jitsuyo Shinan Toroku Koho 1996-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP 2000-11101 A (Hitachi, Ltd.), 14 January, 2000 (14.01.00), Full text; all drawings Full text; all drawings (Family: none)	1,5,9-11,16 2-4,6-7, 12-15,17-19, 21-22
X Y	JP 2-195377 A (Matsushita Electric Ind. Co., Ltd.), 01 August, 1990 (01.08.90), page 1, lower right column, line 14 to page 2, lower left column, line 8; Fig. 4 page 1, lower right column, line 14 to page 2, lower left column, line 8; Fig. 4 (Family: none)	8 2-4,12-13
Y	EP 0949595 A2 (Citicorp Development Center, Inc.), 13 October, 1999 (13.10.99), Par. Nos. [0065] to [0066], [0085], Figs. 2 to 4 & JP, 11-345266, A	6-7,17

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 September, 2000 (18.09.00)	03 October, 2000 (03.10.00)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/04447

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 11-168461 A (NIPPON CONLUX CO., LTD.), 22 June, 1999 (22.06.99), Par. Nos. [0056] to [0079]; Figs. 1 to 3 (Family: none)	13
Y	JP 11-194964 A (Hitachi, Ltd.), 21 July, 1999 (21.07.99), Full text; all drawings (Family: none)	14-15
Y	JP 11-259565 A (Dainippon Printing Co., Ltd.), 24 September, 1999 (24.09.99), Par. Nos. [0013] to [0014], [0018], Fig. 2, 5 to 8 (Family: none)	18-19,21-22

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/04447

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☒ Claims Nos.: 20,23
because they relate to subject matter not required to be searched by this Authority, namely:

The inventions of claims 20, 23 relate to a program stored in an IC card and used for processing and to a computer program, and therefore relate to a subject matter not required to be searched by this Authority according to PCT Article 17(2)(a)(i) and Rule 39.1(vi).

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The inventions of claims 1-13 relate to an IC card wherein information stored in a memory in the IC card is encrypted and decoded using an encryption key so as to back up the information and to a method therefor.

The inventions of claims 14, 15 relate to a method for backing up only altered division units (pages) among information stored in a memory in an IC card.

The inventions of claims 16, 17 relate to a method for realizing backup of information stored in a memory in an IC card as an operating system function.

The inventions of claims 18, 19, 21, 22 relate to a method for storing information from external in an IC card, receiving information representing that information is read in from external, and setting a value in a predetermined area in the IC card.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest ☒ The additional search fees were accompanied by the applicant's protest.
☐ No protest accompanied the payment of additional search fees.

国際調査報告	国際出願番号 PCT／JP00／04447

A. 発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷ G06F17／60, G06K19／07

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷ G06F12／00, G06F12／16, G06F17／60,
G06K17／00, G06K19／07－19／10

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922－1996年
日本国公開実用新案公報 1971－2000年
日本国登録実用新案公報 1994－2000年
日本国実用新案登録公報 1996－2000年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X Y	JP, 2000－11101, A（株式会社日立製作所） 14. 1月. 2000（14. 01. 00） 全文, 全図 全文, 全図 （ファミリーなし）	1, 5, 9-11, 16 2-4, 6-7, 12-15, 17-19, 21-22

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
18. 09. 00	03.10.00
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 相崎 裕恒 5N 2945 電話番号 03－3581－1101 内線 3585

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告	国際出願番号 PCT／JP00／04447

C（続き）． 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X Y	JP，2－195377，A（松下電器産業株式会社） 1．8月．1990（01．08．90） 第1頁右下欄第14行目～第2頁左下欄第8行目，第4図 第1頁右下欄第14行目～第2頁左下欄第8行目，第4図 （ファミリーなし）	8 2-4,12-13
Y	EP，0949595，A2（Citicorp Development Center，Inc.） 13．10月．1999（13．10．99） 【0065】段落～【0066】段落及び【0085】段落，第2－4図 ＆ JP，11－345266，A	6-7,17
Y	JP，11－168461，A（株式会社日本コンラックス） 22．6月．1999（22．06．99） 【0056】段落～【0079】段落，第1～3図 （ファミリーなし）	13
Y	JP，11－194964，A（株式会社日立製作所） 21．7月．1999（21．07．99） 全文，全図 （ファミリーなし）	14-15
Y	JP，11－259565，A（大日本印刷株式会社） 24．9月．1999（24．09．99） 【0013】段落～【0014】段落及び【0018】段落，第2図及び第5－8図 （ファミリーなし）	18-19,21-22

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ００／０４４４７

第Ⅰ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第８条第３項（ＰＣＴ１７条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☒ 請求の範囲 ２０，２３ は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、
請求の範囲２０、２３は、ＩＣカードに格納され、処理を行うプログラムであり、コンピューター・プログラムに該当し、ＰＣＴ１７条(2)(a)(i)及びＰＣＴ規則３９．１(vi)の規定により、この国際調査機関が調査することを要しない対象に係るものである。

2. ☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3. ☐ 請求の範囲 _____ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第３文の規定に従って記載されていない。

第Ⅱ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

請求の範囲１－１３は、ＩＣカード内のメモリに格納されている情報をバックアップするために、暗号鍵を用いて情報の暗号化、復号化を行うＩＣカード及びその方法に関するものである。
請求の範囲１４－１５は、ＩＣカード内のメモリに格納されている情報のうち、変更されている分割単位（ページ）に対してのみバックアップを行う方法に関するものである。
請求の範囲１６－１７は、ＩＣカード内のメモリに格納されている情報のバックアップをオペレーティングシステム機能として実現する方法に関するものである。
請求の範囲１８－１９及び２１－２２は、ＩＣカードに外部から情報を格納する方法であって、外部から読み込まれたことを示す情報を受け取りＩＣカード内の予め定められた領域に値をセットする方法に関するものである。

1. ☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意
☒ 追加調査手数料の納付と共に出願人から異議申立てがあった。
☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。